

ABSTRACT OF THE DISCLOSURE

In an embodiment of the present invention, a technique is provided for remote attestation. An interface maps a device via a bus to an address space of a chipset in a secure environment for an isolated execution mode. The secure environment is associated with an isolated memory area accessible by at least one processor. The at least one processor operates in one of a normal execution mode and the isolated execution mode. A communication storage corresponding to the address space allows the device to exchange security information with the at least one processor in the isolated execution mode in a remote attestation.